基于不完全信息多阶段博弈的入侵路径预测 *

杨峻楠 [1,2]，张红旗 [1,2]，张传富 [1,2]，杨　超 [1,2]

(1. 信息工程大学，郑州 450001; 2. 河南省信息安全重点实验室，郑州 450001)

摘　要：随着入侵的推进入侵者掌握的信息会逐步增加，依据新信息入侵者会找到更好的入侵路径并作出调整。为了使防御方能准确预测入侵路径，首先基于超图理论建立动态防御图并提出动态防御图更新方法，对入侵者的信息更新进行预测；然后建立不完全信息多阶段博弈模型对不同阶段入侵者的入侵路径调整进行预测；最后设计基于博弈的动态防御图路径预测算法，对完整的入侵路径进行预测。实验给出对入侵路径进行预测的典型实例，对实例结果的分析说明了模型的合理性与准确性。

关键词：博弈；防御图；不完全信息；多阶段；路径预测

中图分类号：TP393.08　　doi: 10.3969/j.issn.1001-3695.2017.09.0880

Intrusion path prediction based on incomplete information multi-stage game

Yang Junnan[1,2], Zhang Hongqi[1,2], Zhang Chuanfu[1,2], Yang Chao[1,2]

(1. *Information Engineering University*, *Zhengzhou Henan* 450001, *China*; 2. *Henan Province Key Laboratory of Information Security*, *Zhengzhou* 450001, *China*)

Abstract: The target network information which intruder learn will gradually increase in the intrusion process. According to the new information , intruder will find a better intrusion path than before and adjust strategy. This paper presented a method which can more accurately predict intrusion path. First, it established a dynamic defense graph based on hypergraph theory and proposed the method to update dynamic defense graph. Second, it established incomplete information multi-stage game model. Finally, it designed the dynamic defense graph path predictive algorithm based on game. The experiment gives a concrete example about the model of predicting intrusion path. The reasonableness and accuracy of the model are illustrated by the analysis of the example results.

Keyword: game theory; defense graph; incomplete information; multi-stage; path prediction

0　引言

信息安全事件日趋频繁带来了巨大的损失[1]。研究入侵预测方法，对可能发生的入侵路径进行预测可以弥补防火墙、杀毒软件等传统技术被动防御的缺陷，有效提高系统的安全性。博弈论是研究各博弈方之间策略对抗、竞争对策选择的理论[2]。符合网络入侵者和防御者之间的目标对立性、策略依存性和关系非合作性的特征[3]。将博弈论用于入侵行为预测已经成为一个研究热点。

使用博弈论进行网络安全的研究，博弈信息是一个关键问题。部分学者采用完全信息博弈模型，文献[4]以网络被入侵后所需要的恢复时间作为收益定义完全信息静态博弈模型，并分析了网络安全性。文献[5]采用完全信息动态博弈理论将网络攻击图转换为网络博弈树，用于研究主动防御技术。在网络中，入侵者和防御者存在信息非对称性，双方都无法完全了解对方，使得完全信息博弈模型的应用受到很大的限制。为了解决信息受限的问题，部分学者使用非完全信息博弈模型进行研究。文献[6]建立不完全信息静态博弈模型，并进行漏洞风险分析。虽然文献[6]采用了不完全信息博弈模型，但对入侵行为预测时只进行了一次静态博弈，即认为入侵者在入侵过程中不会改变入侵策略。在实际情况下，入侵者只具有有限的信息收集能力，在入侵之前无法完全了解目标网络，只能依据现有信息制定收益相对高的入侵策略。随着入侵的开展，入侵者会对目标网络有进一步了解，会不断发现更高收益的入侵路径，进而不断调整入侵策略，因此实际的入侵是由不同阶段组成的，入侵者在不同阶段掌握的目标网络信息不同，在每个阶段都会进行策略调整来获取更多的收益。不完全信息动态博弈考虑了入侵者信息更新和策略调整的因素，例如文献[7]建立了攻防信号博弈模

基金项目：国家“863”计划资助项目（2014AA7116082，2015AA7116040）

作者简介：杨峻楠（1993-），男，河北藁城人，硕士研究生，主要研究方向为网络信息安全（624519905@qq.com）；张红旗（1962-），男，河北唐山人，教授，博士，主要研究方向为网络信息安全、计算机应用；张传富（1973-），男，博士（后），主要研究方向为计算机建模、仿真技术；杨超（1988-），男，四川巴中人，博士研究生，主要研究方向为网络信息安全．

型并设计了最优防御策略选取算法，入侵者收到防御者释放的防御信号后会调整入侵策略，但只是对入侵者掌握的防御信号等信息进行了更新，并未对入侵者掌握的目标网络的脆弱性信息进行更新，而脆弱性信息是入侵者制定入侵策略的关键因素，缺少对脆弱性信息的考虑会使得对入侵路径的预测有很大误差。综合以上分析，防御者要想准确预测入侵路径需要解决两个关键问题：一是信息更新的问题。防御者需要对入侵者在不同入侵阶段掌握的脆弱性信息进行预测。目前的博弈模型中，大部分都是以第三方的角度进行分析，以第三方知道攻防双方所有信息为前提，但防御者掌握的信息是受限的，防御者需要科学的方法对入侵者掌握的脆弱性信息的更新进行预测；二是策略调整的问题。每当入侵者掌握了目标网络新的信息后就会调整策略来获取更多收益，防御者需要对每一次入侵者调整的策略进行预测，才能准确预测出最终的入侵路径。

针对上述问题，首先基于超图理论建立动态防御图模型并设计漏洞更新模板建立漏洞更新库，漏洞更新库结合目标环境[8]来对动态防御图进行更新，解决了对入侵者信息更新的预测问题。在此基础上建立不完全信息多阶段博弈模型，对不同阶段入侵者的策略调整进行预测，同时给出了模型具体的求解方法，并设计了基于不完全信息多阶段博弈的动态防御图路径预测算法。

1 动态防御图模型

1.1 动态防御图概念

基于图进行网络安全分析是一个有效的网络安全研究途径。目前图的模型存在两个问题：一、大部分学者使用的图模型只包含入侵的信息[9,10]，缺少了防御的相关信息，不利于网络安全分析。为了全面评估网络安全，姜伟等人[11]在图中引入防御策略节点定义防御图，但防御图只能简单反映入侵路径与防御策略的关系信息，不能反映具体漏洞与相应防御措施的关系。姜伟等人[11]使用二分图描述系统状态与防御策略关系，这种传统图论方法可以表现节点之间的多元关系，但是节点之间的异质性会造成数据连接性、数据聚类等研究与处理过程中的不便[12]。二、目前的图模型都是静态模型。入侵者在入侵过程中会不断加深对目标系统的了解，会因发现更高收益的入侵路径而不断调整入侵策略，这是一个动态过程，静态的图模型无法有效表示这一过程。

综合以上分析，本文首先引入超图理论对其防御图作出改进。Berge[13,14]提出的超图方法既可以很好地表现节点之间的多元关系，还避免了节点的异质性对数据处理带来的困难。将防御图定义为两层模型，上层为入侵者可利用的漏洞，表示入侵者可能的入侵路径，下层为每个漏洞对应的防御措施，使用超图进行描述。然后提出漏洞更新关系定义动态防御图，对入侵过程中入侵者掌握的目标系统的漏洞的更新进行预测。动态防御图具体定义如下：

定义 1 动态防御图(dynamic defense graph) $DDG=\{N,D,L,E\}$，其中：$N=(n_1,n_2,\ldots,n_m)$为漏洞集合，$D=(d_1,d_2,\ldots,d_n)$为防御措施集合。L 为有向边集合，表示漏洞之间的利用关系；D 为超边集合，表示每个漏洞可选用的防御措施。N、D、L 和 E 为动态变化的集合，其中$N=N+f(n_i)$，f表示漏洞间的更新关系，$f(n_i)$为当入侵者渗透漏洞n_i后新加入动态防御图的漏洞，当有新漏洞加入 N 后，需要相应更新集合 D、L 和 E。图 1 为某一状态下的动态防御图示例。

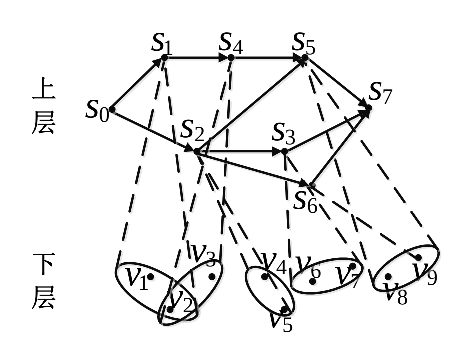


图 1 动态防御图示例

1.2 动态防御图更新

要进行动态防御图更新，关键是确定漏洞间的更新关系f，即：当入侵者渗透一个漏洞节点后，要确定哪些新的漏洞会添加到动态防御图中。目前还没有对漏洞更新关系的研究，本文提出了一种预测漏洞更新的方法。

在 Li 等人[15]的攻击模板模型基础上提出漏洞更新模板模型。通过漏洞更新模板构建漏洞更新库。本文采用 AGML(attack graphs modeling language)建模语言对漏洞更新模板进行形式化描述[16]。漏洞更新模板形式化表示为三元组 VulnerabilityUpdate=< Vul，Pre，Eff>，其中：Vul 为漏洞实体，每个漏洞实体以<VulID，OS，App>描述，VulID 是漏洞的唯一标志符，采用标准的 CVE[17]编号表示；OS 为操作系统信息，采用<OS_name，OS_version>描述，OS_name 为操作系统名称，OS_version 为操作系统版本；App 为应用程序信息，采用<App_name，App_version>描述，App_name 为应用程序名称，App_version 为应用程序版本。

Pre 为漏洞被发现的前提集，Eff 为渗透漏洞的后果集。Pre 和 Eff 使用 AGML 的谓词进行描述。漏洞的探测有两种形式，一种是基于主机的，即漏洞探测者直接登陆目标主机取得一定控制权后，在目标主机上进行漏洞的探测；另一种是基于网络的，即漏洞探测者利用网络远程探测目标主机的漏洞。因此将前提集和后果集都分为主机和网络两部分：Pre=<Pre_host，Pre_net>，Eff=< Eff_host，Eff_net>，其中 Pre_host 和 Pre_net 是“或”的关系，只要满足两者中的一种条件即可探测到此漏洞，但 Pre_host 和 Pre_net 各自内部的谓词之间是“与”的关系。其中具体前提集和后果集见表 1。

目标环境构建是对目标网络中的主机、网络、漏洞等信息进行形式化描述[18]。利用 Sheyner 的目标环境构建方法[8]对目标网络环境进行形式化描述，目标环境结合漏洞更新库即可确

定漏洞间的更新关系 f 。利用 f 更新漏洞集 N,更新 N 后相应更新集合 D、L 和 E 即可完成动态防御图的更新。由于动态防御图的自动构建不是本文的重点，受篇幅限制其构建技术不再详细介绍，后续研究将重点讨论。

表 1　漏洞更新模板前提集和后果集

名称	要素
Pre_host	hasPrivilege(HostID,Privilege),Service(HostID,ServiceName)
Pre_net	trust([HostID,Privilege],[HostID,Privilege]),netConn(HostID,HostID,Protocol,Port),netService(HostID,ServiceName,Protocol,Port)
Eff_host	hasPrivilege(HostID,Privilege)
Eff _net	trust(HostID,HostID,Privilege),netConn(HostID,HostID,Protocol,Port)

2　不完全信息多阶段博弈模型

入侵者往往是序贯理性的[19]，入侵者追求的是最大收益，但是受信息的限制，在入侵刚开始时只能找出当前条件下的最佳入侵路径，而不能直接找出客观上的最佳入侵路径。随着入侵过程中对目标系统了解的不断加深，入侵者会不断向具有更高收益的入侵路径进行调整，即在入侵的不同阶段，入侵者掌握的信息也不同，为了追求本阶段的最大收益，入侵者会在不同阶段进行策略调整。

随着网络安全技术的发展，大部分防御者都能发现本网络所有的漏洞（不包含 0day 漏洞），每个漏洞也都有相应的一个或多个可选防御措施。由于资金和时间等成本的考虑，现实中防御者并不会部署所有可选的防御措施，而且真正对系统有重大威胁的往往只有少数漏洞，因此，防御者会在有限成本下有针对性地进行防御。

对模型作出如下假设：

假设 1　入侵者是贪婪的，总是追求用最少的成本，获得最多的回报。

假设 2　入侵者是理性的，不会为了已获取的权限而发动入侵，其入侵只会向着权限提升的方向发展。

假设 3　入侵者类型为私有信息，但防御者对入侵者类型的概率分布有先验判断，这个先验判断、防御者类型及防御者策略集为入侵者与防御者的共有信息。

假设 4　防御者是智能的，能够发现本网络所有漏洞（不包含 0day）。

假设 5　防御者追求的是“适度安全”，在有限的成本下追求最大的安全收益。

2.1　模型建立

定义 2　不完全信息多阶段博弈模型(incomplete information multi-stage game):

$$IIMG = \{N;S;P;U\}$$

(1) $N = (n_a^j; n_d)$ 是参加博弈的局中人集合，局中人可以是个人也可以是某个有共同利益的团体，大部分对抗可以看成是入侵者 n_a^j 和防御者 n_d 的二人博弈。$n_a^j = (n_a^h; n_a^m; n_a^l)$ 表示入侵者的类型，其中 n_a^h 表示高能力入侵者；n_a^m 表示一般能力入侵者；n_a^l 表示低能力入侵者。

(2) $S = (A, D)$ 是策略集，其中: $A_k = (a_1^k, a_2^k, \ldots, a_n^k)$ 表示入侵方利用漏洞 n_k 进行入侵后入侵方的策略集；$D_k = (d_1^k, d_2^k, \ldots, d_s^k)$ 表示入侵方利用漏洞 n_k 进行入侵后防御方的策略集。

入侵策略就是动态防御图上入侵者当前状态到完成入侵目标的路径。防御策略是入侵路径包含的每个漏洞的防御措施的组合。

(3) $P = (P_0, P_1, \ldots, P_m)$ 是防御方对入侵方类型的先验信念，先验信念可由专家知识获得或由历史经验确定，$P_k = (p_h^k, p_m^k, p_l^k)$ 表示入侵方利用漏洞 n_k 进行入侵后，防御方对入侵方的先验信念，其中 $p_h^k + p_m^k + p_l^k = 1$ 。

(4) $U = (U_a, U_d)$ 表示对抗双方的收益函数，其中：

$$U_{aj}^k = \{u_{a11}^{kj}\left(a_{1j}^k, d_1^k\right), u_{a12}^{kj}\left(a_{1j}^k, d_2^k\right), \ldots, u_{ans}^{kj}\left(a_{nj}^k, d_s^k\right)\}$$

表示入侵方利用漏洞 n_k 进行入侵后入侵方的收益；

$U_{dj}^k = \{u_{d11}^{kj}\left(a_{1j}^k, d_1^k\right), u_{d12}^{kj}\left(a_{1j}^k, d_2^k\right), \ldots, u_{dns}^{kj}\left(a_{nj}^k, d_s^k\right)\}$ 表示防御方的收益。

定义 3　纯策略纳什均衡

在 $IIMG = \{N;S;P;U\}$ 中，策略对 (a_{*j}^k, d_*^k) 是入侵类型为 j 的入侵方利用漏洞 n_k 入侵后进行博弈的一个纳什均衡，则 a_{*j}^k, d_*^k 分别是入侵者和防御者此时的最优策略，即：

$$u_{a**}^{kj}\left(a_{*j}^k, d_*^k\right) \geq u_{ap*}^{kj}\left(a_{pj}^k, d_*^k\right), \forall a_{pj}^k \in A_{kj}, p = 1,2,3,\ldots,n$$

$$u_{d**}^{kj}\left(a_{*j}^k, d_*^k\right) \geq u_{d*q}^{kj}\left(a_{*j}^k, d_q^k\right), \forall d_q^k \in D_s, q = 1,2,3,\ldots,s$$

定义 4　混合策略纳什均衡

在 $MS\text{-}ADG = \{N;S;P;U\}$ 中，入侵者策略集 $A_k = (a_1^k, a_2^k, \ldots, a_n^k)$ 的概率分布为

$$\sigma_a^{kj} = (\sigma_{a1}^{kj}, \sigma_{a2}^{kj}, \ldots \sigma_{an}^{kj}), 0 \leq \sigma_{ap}^{kj} \leq 1, \sum_{p=1}^{n} \sigma_{ap}^{kj} = 1$$

防御者策略集 $D_k = (d_1^k, d_2^k, \ldots, d_s^k)$ 的概率分布为

$$\sigma_d^{kj} = (\sigma_{d1}^{kj}, \sigma_{d2}^{kj}, \ldots \sigma_{ds}^{kj}), 0 \leq \sigma_{dq}^{kj} \leq 1, \sum_{q=1}^{s} \sigma_{dq}^{kj} = 1$$

此时入侵者的期望收益为

$$U_{aj}^k = \sum_{q=1}^{s} \sigma_{dq}^{kj} \left[\sum_{p=1}^{m} \sigma_{ap}^{kj} u_a^{kj}\left(a_p^{kj}, d_q^k\right) \right]$$

此时防御者的期望收益为

$$U_d^i=\sum_{q=1}^{k}\sigma_{dq}^i\left[\sum_{p=1}^{m}\sigma_{ap}^i u_d^i\left(a_p^i,d_q^i\right)\right]$$

如果$\left(\sigma_{a*}^{kj},\sigma_{d*}^{kj}\right)$是一个纳什均衡，则

$$U_{aj}^k\left(\sigma_{a*}^{kj},\sigma_{d*}^{kj}\right)\geq U_{aj}^k\left(\sigma_{a}^{kj},\sigma_{d*}^{kj}\right)\ U_{dj}^k\left(\sigma_{a*}^{kj},\sigma_{d*}^{kj}\right)\geq U_{dj}^k\left(\sigma_{a*}^{kj},\sigma_{d}^{kj}\right)$$

从定义 2 和 3 可以发现，纯策略纳什均衡是一种特殊的混合策略纳什均衡，是某一种策略概率为 1，其余为 0 的混合策略。因此求解结果选用混合策略形式表示。

定义 5　转移概率 t_{er}：表示漏洞 n_e 到漏洞 n_r 的转移概率。

定义 6　被利用概率 t_k :表示漏洞 n_k 被入侵方利用的概率。

入侵路径是由不同漏洞按一定的顺序组在一起的，对入侵路径预测的问题，可以转换成漏洞被利用概率和转移概率求解的问题。当入侵者对某个漏洞渗透成功后，动态防御图会进行更新，可能会有新的漏洞与防御措施补充到动态防御图中，导致入侵策略与防御策略得到更新，从而纳什均衡被打破，双方来到一个新的阶段，要再次进行博弈调整自己的策略。IIMG 模型博弈具体过程如图 2 所示。

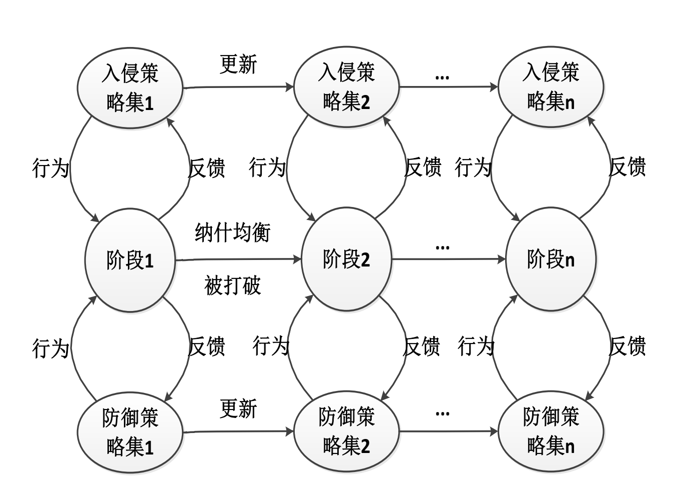


图 2　IIMG 模型博弈过程

2.2　模型求解

2.2.1 纳什均衡求解

纳什均衡的存在性定理（Nash,1950）：每一个有限博弈至少存在一个纳什均衡（纯策略的或混合策略的）[19]。本模型中的每一个非完全信息静态博弈显然是一个有限博弈，因此每次博弈必然存在纳什均衡。

根据收益函数分别得到高能力入侵者、一般能力入侵者、低能力入侵者与防御者之间对应的收益矩阵 M_h、M_m、M_l。

$$M_j=\begin{bmatrix}(u_{a11}^{kj},u_{d11}^{kj}) & (u_{a12}^{kj},u_{d12}^{kj}) & \cdots & (u_{a1s}^{kj},u_{d1s}^{kj})\\ (u_{a21}^{kj},u_{d21}^{kj}) & (u_{a22}^{kj},u_{d22}^{kj}) & \cdots & (u_{a2s}^{kj},u_{d2s}^{kj})\\ \vdots & \vdots & \ddots & \vdots\\ (u_{an1}^{kj},u_{dn1}^{kj}) & (u_{an2}^{kj},u_{dn2}^{kj}) & \cdots & (u_{ans}^{kj},u_{dns}^{kj})\end{bmatrix}$$

将收益矩阵输入博弈工具 Gambit 进行均衡求解，得到混合策略纳什均衡：$\left(\sigma_{a*}^{kj},\sigma_{d*}^{kj}\right)$。

2.2.2 相关概率求解

根据纳什均衡的定义可知，当防御方采取纳什均衡的策略时，入侵方为获得最大收益只能也采取纳什均衡的策略。防御方可据此求得相关概率，对入侵路径进行预测。

转移概率 t_{er}：入侵方会根据纳什均衡选择入侵策略，每个入侵策略的第一个漏洞是入侵者下一步选择渗透的节点，不同入侵策略的第一个漏洞可能相同，此时转移概率需要叠加。当入侵者渗透一个节点后，更新漏洞集合 N，如果有新的漏洞加入 N，代表入侵策略和防御策略都进行了变化，纳什均衡被打破，需要再次求解纳什均衡，此时转移概率求解见式(1)；如果没有新的漏洞加入 N，那么之前的纳什均衡仍然成立，此时可利用之前的纳什均衡结果继续计算转移概率，此时转移概率求解见式(2)。

$$t_{er}=p_h^e*\sum(\sigma_a^{eh}(\mathrm{n}_r))+p_m^e*\sum(\sigma_a^{em}(\mathrm{n}_r))+p_l^e*\sum(\sigma_a^{el}(\mathrm{n}_r))\quad(1)$$

$$t_{er}=\frac{(p_h^e*\sum(\sigma_a^{eh}(\mathrm{n}_r))+p_m^e*\sum(\sigma_a^{em}(\mathrm{n}_r))+p_l^e*\sum(\sigma_a^{el}(\mathrm{n}_r)))*t_s}{t_e}$$

(2)其中：$\sum(\sigma_a^{ej}(\mathrm{n}_r))$ 为所有第一个漏洞为 n_r 的最优策略的概率和；t_s 为求解纳什均衡时所处节点 s 的被利用概率；p_h^e、p_m^e、p_l^e 的值的求解见式(4)~(6)。

被利用的概率 t_r：起始点被利用的概率为 1，其余节点被利用的概率由上一级的所有父节点被利用的概率及其转移概率共同决定。

$$\boldsymbol{t}_r=\sum_e(\boldsymbol{t}_e*\boldsymbol{t}_{er})=$$
$$\sum_e(\boldsymbol{t}_e*(p_h^e*\sum(\sigma_a^{eh}(n_r))+p_m^e*\sum(\sigma_a^{em}(n_r))+p_l^e*\sum(\sigma_a^{el}(n_r))))$$

(3)先验信念 p_r^j：初始状态下防御者对入侵者的先验信念 $P_0=(p_0^h,p_0^m,p_0^l)$ 由历史经验和专家知识获得，在之后的漏洞节点处的先验信念由其上一级的所有父节点的先验信念、被利用的概率及其转移概率共同决定。

$$p_r^h=\frac{\sum_e(t_e*p_h^e*\sum(\sigma_a^{eh}(n_r)))}{\boldsymbol{t}_r}=\frac{\sum_e(t_e*p_h^e*\sum(\sigma_a^{eh}(n_r)))}{\sum_j\sum_e(t_e*p_j^e*\sum(\sigma_a^{ej}(n_r)))}\quad(4)$$

$$p_r^m=\frac{\sum_e(t_e*p_m^e*\sum(\sigma_a^{em}(n_r)))}{\boldsymbol{t}_r}=\frac{\sum_e(t_e*p_m^e*\sum(\sigma_a^{em}(n_r)))}{\sum_j\sum_e(t_e*p_j^e*\sum(\sigma_a^{ej}(n_r)))}\quad(5)$$

$$p_r^l=\frac{\sum_e(t_e*p_l^e*\sum(\sigma_a^{el}(n_r)))}{\boldsymbol{t}_r}=\frac{\sum_e(t_e*p_l^e*\sum(\sigma_a^{el}(n_r)))}{\sum_j\sum_e(t_e*p_j^e*\sum(\sigma_a^{ej}(n_r)))}\quad(6)$$

3　基于不完全信息多阶段博弈的动态防御图路径预测算法

算法是在动态防御图上通过不完全信息多阶段博弈对入侵

路径进行预测。为便于叙述将入侵者作为起始点加入动态防御图中，入侵目标作为目标节点加入动态防御图中，但目标节点不参与博弈分析，如果某一漏洞节点与目标节点直接相连，当入侵者渗透此节点后，即认为入侵者达成入侵目标，此漏洞节点到目标节点的转移概率为 1。

算法 1　基于不完全信息多阶段博弈的动态防御图路径预测算法

Input: 动态防御图 $DDG=\{N,D,L,E\}$，初始先验概率。$P_0=(p_h^0,p_m^0,p_l^0)$，漏洞更新库，目标环境

Output: 转移概率集 T1;被利用概率集 T2。

1）初始化 $IIMG=\{N;S;P;U\}$,$k=0$;

2）do{

3）　构建入侵策略集合 $A_k=(a_1^k,a_2^k,\ldots,a_n^k)$；

4）　构建防御策略集合 $D_k=(d_1^k,d_2^k,\ldots,d_s^k)$；

5）　利用 U_{aj}^k 和 U_{dj}^k 计算不同类型入侵者和防御者在选择不同策略时的收益，然后对应收益矩阵 M_h、M_m、M_l；

6）　利用博弈工具 Gambit 进行均衡求解，得到三个混合策略纳什均衡:

$$\left(\sigma_{a*}^{kh},\sigma_{d*}^{kh}\right)、\left(\sigma_{a*}^{km},\sigma_{d*}^{km}\right)、\left(\sigma_{a*}^{kl},\sigma_{d*}^{kl}\right);$$

7）　do{

8）　　if(在节点 k 进行了纳什均衡求解)

利用式(1)计算漏洞节点 k 到其子节点 r 的转移概率;

else

利用式(2)计算漏洞节点 k 到其子节点 r 的转移概率;

end if

9）　　do{

10）　　利用广度优先算法（*BFS*）选择下一个漏洞节点，更新 k 的值;

11）　　利用 $N=N+f(n_k)$ 更新 N;

12）　　利用式(2)计算漏洞节点 k 的被利用概率;

13）　　利用式(3)~(5)计算先验概率;

14）　　}while(达到入侵目标&&有剩余节点)

15）　if(达到入侵目标&&无剩余节点)

16）　　return *T1, T2*;//算法结束

17）　}while(*N* 未变动)

18）　更新动态防御图 $DDG=\{N,D,L,E\}$；

19）}while(true)

算法 1 采取两个措施减少计算量：a)经过统计大量真实入侵事件发现真实入侵者实施的有效入侵路径的长度绝大部分在 3 以内，且没有发现长度超过 10 以上的[18]，所以剔除长度超过 10 的路径；b)并不是每次入侵后都会有新的漏洞节点加入动态防御图，当动态防御图没有变化时，不重新进行博弈。设算法结束时防御图的漏洞节点数为 n，每个节点双方策略个数为 m，则生成或更新防御图的时间复杂度为 $O(n^4)$，均衡求解的时间复杂度为 $O(n*m^2)$，路径预测算法时间复杂度为 $O(n*m^2+n^4)$。

4　应用实例与分析

4.1　实验环境

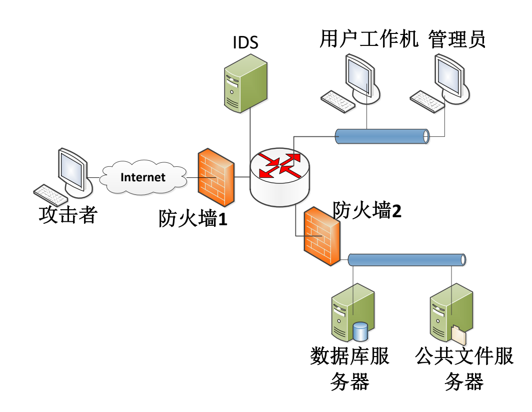


图 3　网络拓扑

本文采用如图 3 所示的典型场景进行实验，该场景便于深入分析信息对入侵者路径选择的影响，适用于验证本算法对路径预测是否合理与准确。入侵者位于外部网络，入侵者与目标网络由防火墙 1 隔开。目标网络共有四台主机，分别为用户主机、管理员主机、共享文件服务器、数据库服务器，其中，防火墙 2 将两台服务器隔离成一个子网。防火墙规则信息如表 2 和 3 所示，各主机的漏洞信息如表 4 所示。防御方的防御措施如表 5 所示。

表 2　防火墙 1 规则信息

源主机	目的主机	访问策略
All	用户主机	Allow
All	管理员主机	Allow

表 3　防火墙 2 规则信息

源主机	目的主机	访问策略
用户主机	共享文件服务器	Allow
管理员主机	共享文件服务器	Allow
管理员主机	数据库服务器	Allow

表 4　各主机漏洞信息

主机	CVE 编号	结果	漏洞编号
用户主机	CVE-2016-3338	root	s_1
管理员主机	CVE-2016-3387	user	s_2
	CVE-2016-3343	root	s_3
共享文件服务器	CVE-2014-1443	root	s_4
数据库服务器	CVE-2015-7564	root	s_5
	CVE-2016-2555	root	s_6

假设入侵者在本机有 root 权限并以取得数据库服务器的 root 权限为入侵目标。由于管理员主机对数据库服务器具有管理权限，所以如果入侵者取得管理员主机 root 权限也视为完成入侵目标。

表 5 防御方策略

防御措施	编号
修改防火墙 1 策略	v_1
修改防火墙 2 策略	v_2
安装漏洞补丁	v_3
隔离主机	v_4
丢弃可疑数据包	v_5
关闭服务	v_6
禁止访问端口	v_7
重启主机	v_8
变更信任关系	v_9

4.2 路径预测

利用算法 1 进行路径预测。将入侵者作为初始节点编号为 s_0，将入侵目标作为目标节点编号为 s_7，入侵者初始漏洞集为 $N=(s_0,s_1,s_2,s_3,s_4,s_5,s_7)$，生成动态防御图如图 4 所示。其中 s_0 被利用概率 $t_0=1$，利用专家知识确定防御者对入侵者的初始先验概率为 P=(0.3,0.4,0.3)。

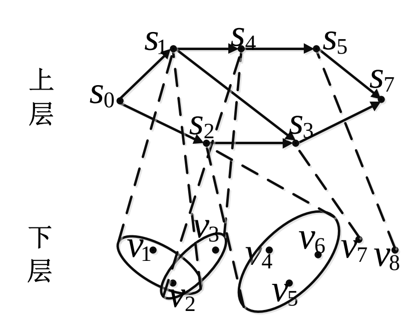


图 4 动态防御图

根据动态防御图可知入侵者入侵策略为

$$a_1^0: s_0\to s_1\to s_3\to s_7$$

$$a_2^0: s_0\to s_1\to s_4\to s_5\to s_7$$

$$a_3^0: s_0\to s_2\to s_3\to s_7$$

防御者防御策略为：

$$d_1^0:\{v_1,v_2,v_3,v_8\}$$

$$d_2^0:\{v_1,v_2,v_7\}$$

$$d_3^0:\{v_4,v_5,v_6,v_7\}$$

利用参考文献[6]的方法进行量化计算，得到收益矩阵：

$$M_h=\begin{bmatrix}(12,5)&(19,7)&(8,12)\\(23,31)&(14,17)&(11,6)\\(3,9)&(8,13)&(13,21)\end{bmatrix}$$

$$M_m=\begin{bmatrix}(13,21)&(15,23)&(6,9)\\(11,23)&(15,17)&(11,9)\\(2,11)&(7,15)&(13,19)\end{bmatrix}$$

$$M_l=\begin{bmatrix}(8,9)&(12,19)&(7,21)\\(7,12)&(11,21)&(13,14)\\(1,11)&(7,17)&(14,22)\end{bmatrix}$$

将收益矩阵输入博弈工具 Gambit 进行均衡求解，得到混合策略纳什均衡：$\sigma_{a^*}^{0h}=(0,0.324,0.676),\sigma_{a^*}^{0m}=(0.75,0.25,0)$ $\sigma_{a^*}^{0l}=(0,0,1)$。利用式(1)计算转移概率:

$$t_{01}=0.3*(0.324+0)+0.4*(0.75+0.25)+0.3*(0+0)=0.497$$

$$t_{02}=0.3*0.676+0.4*0+0.3*1=0.503$$

利用广度优先算法选择下一个漏洞节点 s_1，进行漏洞集更新但没有发生漏洞变动，即纳什均衡没有被打破，利用式(3)计算节点被利用概率：

$$t_1=1*0.497=0.497$$

利用式(4)~(6)计算先验概率：

$$p_1^h=\frac{\sum_e t_e*p_h^e*\sum(\sigma_a^{eh}(i_k))}{t_k}=\frac{1*0.3*(0.324+0)}{0.497}=0.195$$

$$p_1^m=\frac{\sum_e t_e*p_h^e*\sum(\sigma_a^{eh}(i_k))}{t_k}=\frac{1*0.4*(0.75+0.25)}{0.497}=0.805$$

$$p_1^l=\frac{\sum_e t_e*p_h^e*\sum(\sigma_a^{eh}(i_k))}{t_k}=\frac{1*0.3*(0+0)}{0.497}=0$$

由于在 s_1 漏洞没有变动，所以不用重新进行博弈，利用式(2)计算转移概率。

$$t_{13}=\frac{0.3*0+0.4*0.75+0.3*0}{0.497}=0.604$$

$$t_{14}=\frac{0.3*0.324+0.4*0.25+0.3*0}{0.497}=0.396$$

按照广度优先算法选择下一个漏洞节点 s_2，进行漏洞更新。

由于篇幅限制，这里只列出目标环境和漏洞更新模板中与此次漏洞更新相关的内容（表 6、7）。

表 6 目标环境中的主机间连接关系

源主机	目的主机	源主机权限	目的主机访问权限
管理员主机	数据库服务器	user	acess
管理员主机	数据库服务器	root	root
all	管理员主机	root	acess

表 7 漏洞前提集和后果集

漏洞	前提集	后果集
CVE-2016-2555	trust([管理员,user][数据库,acess])	trust([管理员,user][数据库,root])
CVE-2016-3387	trust([入侵者,root][管理员,acess])	trust([入侵者,root][管理员,user])

根据漏洞更新模板和目标环境可知，当入侵者利用 CVE-2016-3387 漏洞入侵管理员主机后会发现 CVE-2016-2555 漏洞存在于数据库服务器中，此时要更新入侵者的漏洞集 $N=(s_0,s_1,s_2,s_3,s_4,s_5,s_6,s_7)$，相应的入侵策略和防御策略发生变

动，纳什均衡被打破，需要进行策略调整。

计算节点被利用概率：

$$t_2 = 1*0.503 = 0.503$$

计算先验概率：

$$p_2^h = \frac{\sum_e t_e * p_h^e * \sum(\sigma_a^{eh}(i_k))}{\mathbf{t}_k} = \frac{1*0.3*0.676}{0.503} = 0.403$$

$$p_2^m = \frac{\sum_e t_e * p_h^e * \sum(\sigma_a^{eh}(i_k))}{\mathbf{t}_k} = \frac{1*0.4*0}{0.503} = 0$$

$$p_2^l = \frac{\sum_e t_e * p_h^e * \sum(\sigma_a^{eh}(i_k))}{\mathbf{t}_k} = \frac{1*0.3*1}{0.503} = 0.597$$

更新动态防御图（图5）：

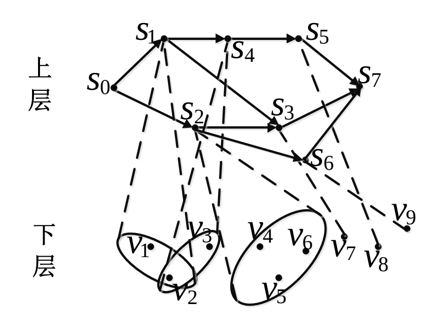


图5　动态防御图

由图5可知入侵者此时的策略为

$$a_1^2 : s_2 \to s_3 \to s_7$$

$$a_2^2 : s_2 \to s_6 \to s_7$$

此时防御方策略为：

$$d_1^2 : \{v_4, v_5, v_6, v_7\}$$

$$d_2^2 : \{v_4, v_5, v_6, v_9\}$$

利用参考文献[6]中进行量化并进行纳什均衡求解得

$$\sigma_{a*}^{2h} = (0.1, 0.9), \sigma_{a*}^{2m} = (0.3, 0.7), \sigma_{a*}^{2l} = (0.2, 0.8)$$

利用式(1)计算转移概率:

$$t_{23} = 0.403*0.1 + 0*0.3 + 0.597*0.2 = 0.16$$

$$t_{27} = 0.403*0.9 + 0*0.7 + 0.597*0.8 = 0.84$$

再按照算法1进行计算，直到算法结束。最终结果如图6所示。

图6　动态防御图上层

其中每个漏洞被利用的概率为

$$t_1 = 0.497, t_2 = 0.503, t_3 = 0.38, t_4 = 0.197, t_5 = 0.197, t_6 = 0.423$$

4.3　结果分析

从结果可以发现，入侵者最有可能的入侵路径为 $s_0 \to s_2 \to s_6 \to s_7$，概率为0.423，其中节点 s_2 被利用的概率为0.503，节点 s_6 被利用的概率为0.423，具有很大的安全隐患。虽然 $s_0 \to s_1 \to s_3 \to s_7$ 和 $s_0 \to s_1 \to s_4 \to s_5 \to s_7$ 两条入侵路径的概率较小，分别为0.3和0.197，但是由于两条路径都经过节点 s_1，使得 s_1 被利用的概率也比较高为0.497，防御者在采取防御措施时不能忽略 s_1 漏洞节点。

使用文献[3,20]的方法进行分析：如果初始漏洞集不包含节点 s_6，由于文献[3,20]的方法不会进行漏洞更新且只进行一次博弈，最终结果会忽略节点 s_6；如果初始漏洞集包含节点 s_6，由于 $s_0 \to s_2 \to s_6 \to s_7$ 入侵路径的高收益，会使得博弈结果偏向这条路径，从而造成节点 s_1 被利用的概率比实际利用的概率要低。在实际中，由于入侵者初始状态信息的缺失，并不能直接准确判断出客观最佳入侵路径 $s_0 \to s_2 \to s_6 \to s_7$，从而造成节点 s_1 也有较高的利用率。通过以上分析，可以发现在这种场景下，本文方法要比文献[3,20]的方法符合实际，更具有合理性与准确性。

为了深入分析信息与入侵路径选择的关系，本实验选择了一个典型场景，随着场景中网络节点数量的增加不会从本质上改变信息对入侵者路径选择的影响，所以本算法在节点数量增加时对入侵路径的预测的合理性与准确性不会改变。网络节点的增加会增加防御图中的节点数，从而造成生成防御图时运算量的增加。本文采用了文献[21]方法生成防御图。文献[21]通过实验验证了该方法能够适用于大型网络，所以本算法在网络节点数量增加时仍然能够适用。

5　结束语

为了对只有有限信息收集能力的入侵者的入侵路径进行预测，首先要对入侵者在不同阶段对目标网络的了解程度进行预测，然后在对不同阶段入侵者的策略调整进行预测。针对上述第一个问题，本文基于超图理论构建动态防御图模型，并给出了动态防御图的更新方法。针对第二个问题，本文在动态防御图上建立不完全信息多阶段博弈模型对不同阶段入侵者的决策进行预测，同时设计了基于不完全信息多阶段博弈的动态防御图路径预测算法。最后通过一个典型的网络实例演示了本文方法在入侵路径预测的具体应用，通过对结果的分析，说明了本方法的合理性与准确性。

为了进一步增加模型的准确性，下一步需要对策略的量化方法进行改进，研究更适合本模型的量化方法。

参考文献：

[1] Liang X, Xiao Y. Game theory for network security [J]. IEEE Communications Surveys & Tutorials, 2013, 15 (1): 472-486.

[2] Fallah M. A puzzle-based defense strategy against flooding attacks using

game theory [J]. IEEE Trans on Dependable & Secure Computing, 2008, 7 (1): 5-19.

[3] 姜伟，方滨兴，田志宏，等. 基于攻防随机博弈模型的防御策略选取研究 [J]. 计算机研究与发展, 2010, 47 (10): 1714-1723.

[4] Lye K W, Wing J M. Game strategies in network security [J]. International Journal of Information Security, 2005, 4 (1-2): 71-86.

[5] 林旺群，王慧，刘家红，等. 基于非合作动态博弈的网络安全主动防御技术研究 [J]. 计算机研究与发展, 2011, 48 (2): 306-316.

[6] 张恒巍，张健，韩继红，等. 基于博弈模型和风险矩阵的漏洞风险分析方法 [J]. 计算机工程与设计, 2016, 37 (6): 1421-1427.

[7] 张恒巍，余定坤，韩继红，等. 基于攻防信号博弈模型的防御策略选取方法 [J]. 通信学报, 2016, 37 (5): 51-61.

[8] Sheyner O M. Scenario graphs and attack graphs [M]. 2004.

[9] Rambo S I, Anka I M. Attack graph-based approach for enterprise networks security analysis [J]. International Journal of Advanced Trends in Computer Science & Engineering, 2016, 5 (5): 16532-16538.

[10] Kumar S, Negi A, Prasad K, et al. Evaluation of network risk using attack graph based security metrics [C]// Proc of IEEE International Conference on Dependable, Autonomic and Secure Computing, International Conference on Pervasive Intelligence and Computing, International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress. 2016: 91-93.

[11] 姜伟，方滨兴，田志宏，等. 基于攻防博弈模型的网络安全测评和最优主动防御 [J]. 计算机学报, 2009, 32 (4): 817-827.

[12] Andersen J L, Flamm C, Merkle D, et al. Maximizing output and recognizing autocatalysis in chemical reaction networks is NP-complete [J]. Journal of Systems Chemistry, 2012, 3 (1): 2012.

[13] Berge C. Graphs and hypergraphs [M]. Amsterdam: North-Holland Publishing Company, 1973.

[14] Berge C. Hypergraphs: combinatorics of finite sets [M]. 1984.

[15] Li Wei. An approach to graph-based modeling of network exploitations [J]. [S. l.] : Mississippi State University, 2005.

[16] 陈锋. 基于多目标攻击图的层次化网络安全风险评估方法研究 [D]. 长沙：国防科学技术大学, 2009.

[17] Common vulnerabilities and exposures [EB/OL]. [2017-7-10]. http://cve. scap. org. cn.

[18] 叶云. 基于攻击图的网络安全风险计算研究 [D]. 长沙：国防科学技术大学, 2012.

[19] 张维迎. 博弈论与信息经济学 [M]. 上海：格致出版社, 2012.

[20] 张健，王晋东，张恒巍，等. 基于节点博弈漏洞攻击图的网络风险分析方法 [J]. 计算机科学, 2014, 41 (9): 169-173.

[21] 叶云，徐锡山，齐治昌，等. 大规模网络中攻击图自动构建算法研究 [J]. 计算机研究与发展, 2013, 50 (10): 002133-2139.